

EXHIBIT 48

JAMS COMMERCIAL ARBITRATION TRIBUNAL

GEMINI TRUST COMPANY, LLC,

Claimant,

v.

SHANE MOLIDOR,

Respondent.

Ref. No. 1425025351

Arbitrator: Mark E. Segall

**AFFIDAVIT OF SHANE
MOLIDOR**

STATE OF NEW YORK)
) ss.;
COUNTY OF NEW YORK)

SHANE MOLIDOR, being duly sworn, deposes and says:

1. I make this affidavit based on the facts as I can best recall them and my review of relevant documents.

2. On January 20, 2016, I began my employment with Gemini Trust Company, LLC ("Gemini") as a Customer Support Specialist.

3. In around December 2016, I took over some of the responsibilities of Daniel Kim, who had been Gemini's Director of Institutional Sales. I officially began reporting to Benjamin Small in around March 2017, when he became Gemini's Chief Operating Officer. As part of my duties, I negotiated bespoke fee agreements with high volume market participants across Gemini's three order books: the BTC/USD order book, the ETH/USD order book, and the ETH/BTC order book.

4. I negotiated fee arrangements for, among others, Cardano Singapore PTE Ltd. ("Cardano") and Hashtech, LLC ("Hashtech"), who were extended some of the best terms of any

#72606v1

DX 706

market participants on Gemini's three order books.

5. On around March 21, 2017, I negotiated and subsequently offered Cardano a 15bps maker rebate and a 5bps taker fee across Gemini's three order books. I received approval for this bespoke fee arrangement from my supervisor, Benjamin Small.

6. On around March 21, 2017, I negotiated and subsequently offered Hashtech a 15bps maker rebate and a 5bps taker fee on Gemini's ETH/USD and ETH/BTC order books, and a 5bps maker rebate and a 15bps taker fee on Gemini's BTC/USD order book. On around June 1, 2017, I negotiated an adjustment of Hashtech's fee arrangement to a 15bps maker rebate and a 5bps taker fee on all three of Gemini's order books. On around June 27, 2017, I again negotiated an adjustment to Hashtech's fee arrangement to a 12bps maker rebate and a 2bps taker fee across all three of Gemini's order books.

7. I received approval for these bespoke fee arrangements and adjustments from my supervisor, Benjamin Small.

8. Gemini's Chief Compliance Officer Michael Breu, Cameron Winklevoss, and Tyler Winklevoss never approved these agreements.

9. Cardano and Hashtech trading against each other (i.e., cross trades) resulted in a net loss to Gemini, because their maker rebates exceeded their taker fees.

10. Benjamin Small and I discussed that losses were incurred where certain maker rebates exceeded taker fees. As early as May 8, 2017, Mr. Small was aware that Cardano and Hashtech had traded against one another about 75% of the time on Gemini's ETH/BTC order book the prior weekend, resulting in losses, after software engineer Noah Cornwell raised the issue.

11. Despite previous losses incurred due to Cardano and Hashtech cross trades, Mr. Small approved an extension of Hashtech's fee arrangement at the beginning of May and an

extension of Cardano's fee arrangement at the end of May. Neither of these extensions were explicitly stated on the #market-makers Slack channel. I did not discuss this with Cameron Winklevoss, Tyler Winklevoss, or Michael Breu.

12. I had another conversation with Mr. Small in early July 2017 about losses incurred as a result of cross trading between clients with high maker rebates and low taker fees after Noah Cornwell again pointed out in the #market-makers Slack channel that Gemini was losing money on trades.

13. I did not bring the issue of losses incurred by cross trading between Cardano and Hashtech to the attention of Cameron Winklevoss, Tyler Winklevoss, or Michael Breu at the time.

14. The first time I had a conversation with Cameron Winklevoss, Tyler Winklevoss, or Michael Breu about the Cardano-Hashtech losses was on August 23, 2017, when Cameron Winklevoss asked me why Gemini had incurred losses equal to 113 bitcoin in July.

15. The Key Performance Indicators ("KPIs") that I compiled during the course of 2017 for presentation to Gemini's Board of Managers did not mention the losses sustained by Gemini related to cross trading between Cardano and Hashtech.

16. As part of my responsibilities, at the direction of Cameron Winklevoss I helped negotiate the terms of bitcoin and ether loans made by Pearl Street Financial, LLC ("Pearl Street"). Mr. Small was included in many communications concerning Pearl Street and its activities and was familiar with the terms extended to many of Gemini's market participants that received Pearl Street loans. For example, in an email communication dated December 1, 2016 from Max Boonen of B2C2 Ltd. to Small, Mr. Boonen discussed, among other things, Pearl Street's 1000 BTC loan to B2C2 and their request for an increase on another BTC loan. Further, Mr. Small sent me a message on January 4, 2017 that, if XBT Opps, LLC (a Gemini market participant) ("XBTO") was


capital-constrained, Cameron and Tyler Winklevoss could help, implying a potential extension of a Pearl Street loan. Similarly, on July 3 and 4, 2017, Mr. Small, Sarah Olsen and I discussed, via a Slack channel communication, Sonar Trading's request for a Pearl Street loan. In addition, Mr. Small joined me and Cameron Winklevoss on calls with loan recipients XBTO, B2C2, and Circle Financial, Inc.

17. On several occasions, I arranged for Gemini to extend operational advances to market participants. It was my understanding of company policies and procedures (attached) that market participants were expected to send corresponding funds for these advancements to be delivered to Gemini within approximately 24 hours. I never advised Cameron or Tyler Winklevoss of any situation where operational advances did not comply with company policies and procedures. I was never advised by Cameron or Tyler Winklevoss that it was permissible for operational advances to remain outstanding in a manner that was not consistent with company policies and procedures.

Dated: June 24, 2021
New York, New York


SHANE MOLITOR

Sworn before me on this 24 day
of June, 2021


Notary Public

• TODD A. GUTFLEISCH
Notary Public, State of New York
No. 02GU5039698
Qualified in Nassau County
Commission Expires February 21, 2023

CONFIDENTIAL

Last revised - May 21, 2017



**GEMINI TRUST COMPANY, LLC
POLICIES AND PROCEDURES MANUAL
FUNDS TRANSFER, LEDGER, AND CUSTODY
CONFIDENTIAL**

Gemini Trust Company, LLC - Policies and Procedures - Funds Transfer, Ledger, and Custody

1

Confidential Treatment Requested by Gemini Pursuant to FOIA

GEM_CFTC374018

CONFIDENTIAL

Last revised - May 21, 2017

Table of Contents

INTRODUCTION	4
Purpose of This Manual	5
Employee Responsibilities	5
How to Use This Manual	6
FUNDS TRANSFER	7
Approval Groups	7
Approval Design — Deposits	8
Approval Design — Operational Advances	8
Approval Design — Withdrawals	9
Approval Design — Whitelisting	9
Approval Design — ACH Limits	10
Approval Design — Bank Accounts	10
Settlement — Digital Asset Deposits	11
Settlement — ACH Deposits	11
Settlement — Wire Deposits	12
Settlement — Digital Asset Withdrawals	12
Settlement — ACH Withdrawals	13
Settlement — Wire Withdrawals	14
Digital Asset Address Creation and Monitoring	15
Digital Asset Address Whitelisting	15
Withdrawal Delay Notification	15
Cancellation of Funds Transfer	15
Bank Transaction Settlement Time	16
Employee Fingerprinting and Background Checks	16
CUSTODY OF FIAT FUNDS	17
Principal Bank	17
Omnibus Bank Account Review	17
CUSTODY OF DIGITAL ASSETS	18
Three-Tiered Storage System	18
Digital Asset Allocation	19
Segregated Account Management	19
Storage Facility Access / Operation of Signers	19
Storage Facility Review	20
Proof of Control	20
TOKEN HOLDER POLICY	21

Gemini Trust Company, LLC - Policies and Procedures - Funds Transfer, Ledger, and Custody

2

CONFIDENTIAL

Last revised - May 21, 2017

Appointment and Termination	21
Responsibilities	21
Participation in Operations	23
Access Controls	23
Storage Facility Log	23
Confidentiality	23
Transfer of Token Custody	23
Amendments	24
Certification	24
EXCHANGE LEDGER	25
Approval Groups	25
Approval Design	25
Pooled Accounts	25
Securing, Maintaining and Backing Up	26
Records	26
Backups	26
TRADE ERRORS & MODIFICATIONS	27
Approval Groups	29
Approval Design	29
Discovery & Reporting of Errors	29
Reporting to Users	29
Pre-Settlement Correction	29
Post-Settlement Correction	29
Appendix 1: Initial Certification	30
Appendix 2: Annual Certification	31
Appendix 3: Token Holder Certification	32

CONFIDENTIAL

Last revised - May 21, 2017

INTRODUCTION

Gemini Trust Company, LLC, a New York State-chartered limited purpose trust company (herein "our Organization"), operates an exchange and custody business (collectively, "Gemini"), whereby our exchange ("Exchange") facilitates the purchase or sale of Digital Assets¹ (e.g., bitcoin or ether) in exchange for fiat currency (e.g., U.S. Dollars) or Digital Assets, and our custodial service ("Cold Storage System") securely stores Digital Assets. Gemini's online platform ("Online Platform") services both individual and institutional customers (each, a "User") and allows buyers and sellers to make offers to buy and/or sell Digital Assets at a given price, a record of which offers are maintained in Gemini's order book ("Order Book"). When the exchange trading engine ("Exchange Trading Engine") used by Gemini matches buy and sell offers on the Order Book, Gemini records the trade in its ledger ("Exchange Ledger"), effectively transferring ownership of the selling User's traded Digital Assets to the buying User, and ownership of the related purchase price in fiat currency from the buying User to the selling User. Changes in ownership of Digital Assets and fiat currency are recorded in the Exchange Ledger and are reflected in a User's Digital Asset account ("Digital Asset Account") and fiat account ("Fiat Account").

Our Organization has agreements with one or more FDIC-insured depository institutions (each, a "Bank") to hold custody of fiat currency in a one or more omnibus bank accounts (each, an "Omnibus Bank Account"), each of which is a bank account in the name and under the control of our Organization. While we do not directly handle User fiat currency, we (i) maintain sub-accounts for each User on our Exchange Ledger, which are reflected in a User's Fiat Account and we (ii) control the flow of User fiat currency by providing instructions on the movement of such funds to banks. A User's Fiat Account does not represent a banking relationship with the Bank(s), and a User does not have direct control over the fiat currency deposited in our Omnibus Bank Account(s).

Our Organization holds custody of Digital Assets in a User's Digital Asset Account. Users transfer Digital Assets into either (i) a pooled Digital Asset account ("Pooled Account"), secured and maintained by our Organization, that does not allocate specific units of Digital Assets to Users (i.e., a User does not have a claim to a specific Digital Asset, but rather to that number of Digital Assets drawn from the pool), or (ii) a segregated custody account, the balances of which are recorded in our Exchange Ledger and reflected in a User's Digital Asset Account. When a User requests a withdrawal from their Digital Asset Account, we process the withdrawal instructions if they are valid. Secure storage of Digital Assets is achieved through a design that utilizes offline storage (i.e., Cold storage and "Cryo" storage, collectively our Cold Storage System).

¹ "Digital Asset" means a digital asset (also called a "cryptocurrency," "virtual currency," "digital currency," or "digital commodity"), such as bitcoin or ether, which is based on the cryptographic protocol of a computer network that may be (i) centralized or decentralized, (ii) closed or open-source, and (iii) used as a medium of exchange and/or store of value.

CONFIDENTIAL

Last revised - May 21, 2017

Purpose of This Manual

Our Organization is committed to the highest legal and ethical standards in the Digital Asset exchange and custody industry. It is the responsibility of every employee and officer (each, an "Employee" or "you") of our Organization to fulfill this commitment to ethical conduct and compliance with laws and regulations. The Employees of our Organization have a responsibility to act in accordance with this policies and procedures manual ("Manual") in the operation of Gemini.

This Manual has been adopted by our Organization to ensure that Employees are aware of the expectations and rules for the operation related to funds transfer and custody, and to ensure the smooth and accurate transfer of funds to and from and between Users.

Employee Responsibilities

As a matter of Organization policy, compliance with this Manual is a condition of continued employment with our Organization. Failure to comply with any policies and procedures in this Manual may result in disciplinary action against the Employee, including but not limited to a warning, fine, disgorgement, suspension, or termination of employment. In addition to sanctions imposed by our Organization, violations may be referred to civil or criminal authorities where appropriate.

The CCO, in consultation with senior management, reviews, at least annually, the Funds Transfer, Ledger, and Custody Policy and, in light of any security and operational developments as well as experience gained through implementation, makes any appropriate changes.

Each Employee who is involved in funds transfer must sign the Initial Certification, attached hereto as **Appendix 1**, certifying that he or she has read and understood this Manual and will comply with its requirements in all respects.

Each Employee who is involved in funds transfer is required to, at least annually, sign the Annual Certification, attached hereto as **Appendix 2**, certifying that he or she has been and will continue to be in compliance with this Manual and its requirements in all respects.

All Employees who are designated as custodians for our Cold Storage System must sign the Token Holder Policy, attached hereto as **Appendix 3**.

The CCO is responsible for ensuring that every Employee signs all his or her required certifications.

CONFIDENTIAL

Last revised - May 21, 2017

This Manual is the property of our Organization and its contents are ***strictly confidential***. Each Employee must return his or her copy of this Manual to the CCO upon termination of employment for any reason.

How to Use This Manual

Generally, for each topic, a summary of our Organization's policy will be followed by procedures that implement our policy. Use of the word "we" or "our" in this Manual refers to our Organization and all of our Employees.

CONFIDENTIAL

Last revised - May 21, 2017

FUNDS TRANSFER

Policy

Funds Transfer. It is the policy of our Organization to utilize controls and procedures regarding the deposit, withdrawal and transfer of User funds.

Approval. Certain funds transfers require approval by one or more Employees that are members of distinct approval groups (each, an "Approval Group") with role-specific privileges.

Prompt Settlement. Prompt settlement of User deposits and withdrawals is a priority of our Organization. We will notify affected Users if settlement of a deposit or withdrawal is delayed.

Procedures

Approval Groups

Gemini Admin — Certain Employees have access to our administrative system ("Admin"). These Employees are members of one or more Approval Groups as defined below:

- **Management** — Our President, Chief Executive Officer ("CEO"), Chief Compliance Officer ("CCO"), and Chief Operating Officer ("COO");
- **Support** — Employees who are customer support generalists and who do not have specific compliance or cash management responsibilities;
- **Inbound Wire Approver** — Employees who manage User fiat deposits and withdrawals to and from our Omnibus Bank Account(s) via Automated Clearing House ("ACH") or bank wire ("Wire") transfers in the cash management module of Admin (the "Cash Module");
- **Compliance** — Employees who perform the compliance functions of User onboarding, account risk review, and account monitoring, among other responsibilities; and
- **Compliance Auditor** — Examiners and auditors who have visibility into Admin for a limited time period with read-only access.

Bank Module — Certain Employees have access to the Silvergate Bank platform ("Bank Module"). These Employees are members of one or more Approval Groups as defined below:

- **Outbound Wire Initiator** — Employees who are able to setup outbound Wires on the Bank Module.

CONFIDENTIAL

Last revised - May 21, 2017

- **Outbound Wire Approver** — Employees who are able to approve outbound Wires on the Bank module.
- **Outbound Wire Template Initiator** — Employees who are able to setup an outbound Wire template on the Bank module.
- **Outbound Wire Template Approver** — Employees who are able to approve an outbound Wire template on the Bank module.

Approval Design — Deposits

The following approvals are required for User deposits:

- A **deposit** of Digital Assets requires a User to authenticate to our Online Platform and obtain a Digital Asset deposit address associated with his or her Gemini account ("Gemini Account"). No approval is required.
- A **deposit** of fiat funds via Automated Clearing House ("ACH") transfer requires a User to authenticate to our Online Platform and submit an ACH transfer request. No approval is required.
- A **deposit** of fiat funds via Wire requires a User to authenticate to our Online Platform and generate Wire instructions. Upon receipt of funds, the following approvals are required:
 - If a Wire (and the aggregate amount of Wires sent by a User in past 24 hours) is < \$20,000.00, it must be approved by one (1) **Inbound Wire Approver**.
 - If a Wire (or the aggregate amount of Wires sent by a User in past 24 hours) is ≥ \$20,000.00, it must be approved by two (2) **Inbound Wire Approvers**.
 - If a Wire requires an **adjustment**, such adjustment must be submitted by one (1) **Inbound Wire Approver** on the Cash Module and approved by one (1) additional **Inbound Wire Approver**.

Approval Design — Operational Advances

An **operational advance** for a Wire deposit may be provided to select institutional Gemini Accounts in an effort to bridge an incoming Wire deposit, if the registered User(s) of such a Gemini Account can provide proof that their Wire is in transit (e.g., wire transfer confirmation, Fedwire reference number, etc.). The time period for an operational advance does not typically

CONFIDENTIAL

Last revised - May 21, 2017

exceed twenty four (24) hours. If a Gemini Account is extended an operational advance, that Gemini Account can immediately trade the full value of such advance; however, a withdrawal hold is put on the Gemini Account in an amount equal to or greater than the amount of the operational advance while the funds are in transit, thereby preventing withdrawals in excess of the actual Gemini Account asset balance. When the funds in transit are received and considered settled, the withdrawal hold is removed from the Gemini Account.

The following approval are required for an operational advance of a User's wire deposit:

- An **operational advance** of a Wire must be approved by one (1) **Inbound Wire Approver**, which will immediately credit the Wire amount to the User's Fiat Account while the funds are still in transit, and place a withdrawal hold on the User's Gemini Account in an amount equal to or greater than the Wire. Once the Wire has been received, one (1) additional **Inbound Wire Approver** can release the withdrawal hold placed on the User's Gemini Account.

Approval Design — Withdrawals

The following approvals are required for User withdrawals:

- A **withdrawal** of Digital Assets requires a User to authenticate to our Online Platform and perform an additional second factor authentication ("2FA") at the time of submitting a Digital Asset withdrawal request. No approval is required.
- A **withdrawal** of fiat funds via ACH transfer requires a User to authenticate to our Online Platform and perform an additional 2FA authentication at the time of submitting an ACH transfer withdrawal request. No approval is required.
- A **withdrawal** of fiat funds via Wire requires a User to authenticate to our Online Platform and perform an additional 2FA authentication at the time of submitting a Wire withdrawal request. Once submitted, an outbound Wire requires the following approvals:
 - An outbound Wire must be submitted to the Bank Module by one (1) **Outbound Wire Initiator** and approved by one (1) **Outbound Wire Approver**; and
 - An outbound Wire Template can be setup for a User in the Bank Module by one (1) **Outbound Wire Template Initiator**, but must be approved by one (1) **Outbound Wire Template Approver**.

Approval Design — Whitelisting

The following approvals are required for whitelisting a User's Digital Asset:

Gemini Trust Company, LLC - Policies and Procedures - Funds Transfer, Ledger, and Custody

9

CONFIDENTIAL

Last revised - May 21, 2017

- **Whitelisting** of a Digital Asset withdrawal address for a User's Gemini Account can be performed by any (1) member of the **Compliance** or **Support** group.

All approval actions, as described above, are recorded and visible to Employees with Admin access.

Approval Design — ACH Limits

The following approvals are required for adjusting a User's ACH Limit:

- An **ACH Limit Adjustment** can be submitted by any (1) Employee with **Admin** access, but must be approved by one (1) member of the **Management** group.

Approval Design — Bank Accounts

The deposit and withdrawal of User fiat funds to and from our Omnibus Bank Account(s) involves ACH or Wire transfers between our Omnibus Bank Account(s) and a User's bank account, which has **successfully completed our bank account verification process** (each, a "User Bank Account").

- We will not initiate an ACH pull request from or push request to any bank account that has not successfully completed our bank account verification process.
- We will not initiate a Wire transfer to any bank account that has not successfully completed our bank account verification process.
- We will reject or return any funds sent via Wire or ACH transfer to our Omnibus Bank Account(s) that has not originated from a User Bank Account, unless at least one (1) member of the **Compliance** group and one (1) member of the **Management** group have approved the funds transfer as being in compliance with our Bank Secrecy Act and Anti-Money Laundering ("BSA/AML") Compliance Program (collectively, "BSA/AML Program").

CONFIDENTIAL

Last revised - May 21, 2017

Settlement — Digital Asset Deposits

A User, upon completing our BSA/AML Program, may deposit Digital Assets into any Digital Asset deposit address associated with his or her Gemini Account.

- **Initiation** — For a Digital Asset deposit, a User (i) authenticates to our Online Platform; (ii) obtains a Digital Asset deposit address associated with his or her Gemini Account (if they have not already done so); and (iii) initiates a Digital Asset transaction to one of his or her Gemini Digital Asset deposit addresses.
- **Settlement** — In the case of bitcoin, a deposit is considered settled after two (2) blocks have been added to the Blockchain following the initial block that recorded the deposit in the Blockchain (i.e., after three (3) "confirmations"). Digital Asset deposits are recorded in our Exchange Ledger and credited to a User's Digital Asset Account immediately after settlement. Settlement and confirmation times for other Digital Assets may vary. Our Chief Compliance Officer ("CCO") may adjust the Digital Asset deposit settlement parameters for a given Digital Asset and/or User.
- **Availability** — At the discretion of our Organization, Digital Asset deposits can be made immediately available to Users for trading prior to the completion of the settlement cycle described above; however a withdrawal hold is put on the User's Gemini Account in an amount equal to or greater than the amount of the Digital Asset deposit while the funds are in transit, thereby preventing withdrawals in excess of the User's actual Gemini Account asset balance. When the funds in transit are considered settled, the withdrawal hold will be removed from the User's Gemini Account.

Settlement — ACH Deposits

A User, upon completing our BSA/AML Program, may deposit fiat funds into his or her Fiat Account via ACH deposit transfer from his or her User Bank Account(s).

- **Initiation** — For an ACH deposit transfer, a User (i) authenticates to our Online Platform; (ii) fills out a deposit authorization form that specifies the amount of funds to be deposited; and (iii) authenticates again using 2FA to confirm the ACH deposit transfer request.
- **Settlement** — ACH deposit transfers are considered settled three (3) business days after we have instructed our Bank to initiate an ACH "pull" transaction from a User's Bank Account to our Omnibus Bank Account, since by this time the bulk of ACH return or reversal risk has passed. An ACH deposit transfer which is returned or reversed may lead to a User having a negative Fiat Account balance. The ACH system utilized by our

CONFIDENTIAL

Last revised - May 21, 2017

Bank(s) and our User's Bank(s) determines the settlement cycle of ACH deposit transfers.

- **Availability** — ACH deposit transfer funds are made immediately available to Users for trading prior to the completion of the settlement process described above; however, a withdrawal hold is put on the User's User's Gemini Account in an amount equal to or greater than the amount of the ACH deposit transfer while the funds are in transit, thereby preventing withdrawals in excess of the User's actual Gemini Account asset balance. When the funds in transit are considered settled, the withdrawal hold will be removed from the User's Gemini Account.

Settlement — Wire Deposits

A User, upon completing our BSA/AML Program, may deposit fiat funds into his or her Fiat Account via Wire deposit from his or her User Bank Account(s).

- **Initiation** — For a Wire deposit, a User (i) authenticates to our Online Platform; (ii) specifies the amount of funds to be deposited thereby generating a Wire deposit slip; (iii) our Online Platform displays the Wire instructions of our Omnibus Bank Account to the User; and (iv) the User initiates a Wire deposit from his or her User Bank Account to our Omnibus Bank Account.
- **Settlement** — Wire deposits settle immediately once they have been received in our Omnibus Bank Account. Once approved by the requisite number of Inbound Wire Approvers, unless earlier approved (See operational advance above), our Exchange Ledger updates automatically, which credits the User's Fiat Account balance in the amount of the Wire deposit. The FedWire system utilized by our Bank(s) and our User's Bank(s) determines the settlement cycle for Wire deposits.
- **Availability** — Wire deposits funds are made available to Users for trading and withdrawal shortly after they have been received in our Omnibus Bank Account. In the case of a Wire deposit, a withdrawal hold is never placed on a User's Gemini Account because Wire deposits settle immediately and are unable to be reversed.

Settlement — Digital Asset Withdrawals

A User, upon completing our BSA/AML Program, may withdraw Digital Assets to any Digital Asset deposit address that the User specifies.

- **Initiation** — For a Digital Asset withdrawal, a User (i) authenticates to our Online Platform; (ii) fills out a Digital Asset withdrawal authorization form that specifies the

CONFIDENTIAL

Last revised - May 21, 2017

amount of funds to be withdrawn and the destination Digital Asset address; and (iii) authenticates again using 2FA to confirm the Digital Asset withdrawal request.

- **Settlement** — Upon receipt of a Digital Asset withdrawal request, we automatically (i) check to ensure a User has sufficient funds in his or her Digital Asset Account to satisfy the Digital Asset withdrawal request; (ii) place a "hold" on the required funds to satisfy the withdrawal (i.e., making the required funds available only to satisfy the Digital Asset withdrawal request or rejecting the request if it's greater than funds available); (iii) initiate the Digital Asset withdrawal via Digital Asset transaction from the User's Digital Asset Account to the Digital Asset address specified by the User; and (iv) update our Exchange Ledger, which debits the User's Digital Asset Account balance in the amount of the Digital Asset withdrawal.
- **Instructions** — Absent extraordinary circumstances, such as the depletion of the Hot wallet requiring the manual retrieval of Digital Assets from our Cold Storage System, our automated system (or multiple Token Holders as defined below, if required) automatically initiates a Digital Asset transaction from our Hot wallet immediately upon the generation of a valid request. A Digital Asset withdrawal involves the transmission of available Digital Assets from our Hot wallet to a User's specified Digital Asset deposit address and is conducted on a near real-time basis if we have sufficient Digital Assets in our Hot wallet. If we lack sufficient Digital Assets in our Hot wallet (i.e., an instance whereby the amounts of Digital Asset withdrawal requests exceed the amount of Digital Asset reserves held in our Hot wallet at that point in time to satisfy such requests), we may delay the settlement of Digital Asset withdrawal requests until we are able to retrieve additional Digital Assets from our Cold Storage System or until additional Digital Assets become available in our Hot wallet from the deposit of Digital Assets by other Users.

Settlement — ACH Withdrawals

A User, upon completing our BSA/AML Program, may withdraw fiat funds from his or her Fiat Account via ACH withdrawal transfer to his or her User Bank Account(s).

- **Initiation** — For an ACH withdrawal transfer, a User (i) authenticates to our Online Platform; (ii) fills out an ACH withdrawal transfer authorization form that specifies the amount of funds to be withdrawn and the destination User Bank Account; and (iii) authenticates again using 2FA to confirm the ACH withdrawal transfer request.
- **Settlement** — Upon receipt of an ACH withdrawal transfer request, we automatically (i) check to ensure a User has sufficient funds in his or her Fiat Account to satisfy the ACH withdrawal transfer; (ii) place a "hold" on the required funds to satisfy the withdrawal (i.e., making the required funds available only to satisfy the ACH withdrawal transfer request

CONFIDENTIAL

Last revised - May 21, 2017

and or rejecting the request if it's greater than the funds available); (iii) initiate the ACH withdrawal transfer via ACH "push" transaction from our Omnibus Bank Account to the User's Bank Account; and (iv) update our Exchange Ledger, which debits the User's Fiat Account balance in the amount of the ACH withdrawal transfer.

- **Instructions** — Our automated system (or an Employee authorized to give instructions to our Bank(s)) instructs our Bank to initiate an ACH "push" transaction usually on the same business day and no later than the next business day following the generation of a valid request.

Settlement — Wire Withdrawals

A User, upon completing our BSA/AML Program, may withdraw fiat funds from his or her Fiat Account via Wire withdrawal to his or her User Bank Account(s).

- **Initiation** — For a Wire withdraw, a User (i) authenticates to our Online Platform; and (ii) fills out a Wire withdrawal authorization form that specifies the amount of funds to be withdrawn and the destination User Bank Account.
- **Settlement** — Upon receipt of a Wire withdrawal request, we automatically (i) check to ensure a User has sufficient funds in his or her Fiat Account to satisfy the Wire withdrawal and (ii) place a "hold" on the required funds to satisfy the withdrawal (i.e., making the required funds available only to satisfy the Wire withdrawal request and or rejecting the request if it's greater than the funds available). Once the Wire withdrawal funds have been debited from our Omnibus Account, we update our Exchange Ledger, which debits the User's Fiat Account balance in the amount of the Wire withdrawal transfer.
- **Instructions** — Our automated system (or an Outbound Wire Initiator sets up the Wire in the Bank Module to be approved by an Outbound Wire Approver)) instructs our Bank to initiate a Wire transaction on the same business day of the generation of a valid request.

CONFIDENTIAL

Last revised - May 21, 2017

Digital Asset Address Creation and Monitoring

- **Creation of Addresses** — We create unique Digital Asset deposit addresses for each User's Gemini Account.
- **Monitoring of Addresses** — We monitor all Digital Asset deposit addresses uniquely assigned to a User's Gemini account. We also monitor all Digital Asset addresses of our Organization.

Digital Asset Address Whitelisting

- **Whitelisting for Withdrawals** — A User may request to restrict all withdrawals from his or her Digital Asset Account to one or more specific Digital Asset Addresses (i.e., a "whitelist"). We will authenticate and implement such whitelist requests. Users who have successfully setup whitelisting will not be permitted to withdraw Digital Assets to a non-whitelisted Digital Asset address. Whitelisting is primarily setup as a safety measure to protect a User's Digital Asset holdings in the event that his or her Gemini Account becomes compromised.
- **Whitelisting for Gemini** — We restrict all withdrawals from our Cold Storage System to our Hot wallet Digital Asset addresses. All Hot wallet Digital Asset addresses have been whitelisted to our Cold Storage System. Digital Assets are not permitted to be withdrawn from our Cold Storage System to a non-whitelisted Digital Asset address (i.e., Digital Asset Addresses other than our Hot Wallet Digital Asset addresses).

Withdrawal Delay Notification

In the event that settlement of a withdrawal is delayed in excess of twenty-four (24) hours, we will notify the affected Users of such delay.

Cancellation of Funds Transfer

In the event that the **Management** group or the CCO determines that a funds transfer lacks proper authority or may otherwise violate our policies and/or procedures, he or she, may (i) place a hold on the transfer (i.e., delay settlement); (ii) notify the User of such a hold and request additional information, if necessary; and (iii) provide the User with a Customer Service Team telephone number or email address to discuss the hold on the funds transfer. If the User does not respond to the additional inquiry within five (5) business days, the funds transfer will be cancelled.

In the event that the **Management** group or the CCO determines that a funds transfer violates our BSA/AML Program, or may constitute illegal activity and/or require the filing of a SAR, we (in

Gemini Trust Company, LLC - Policies and Procedures - Funds Transfer, Ledger, and Custody

15

CONFIDENTIAL

Last revised - May 21, 2017

accordance with our BSA/AML Program) *will not* inform any User or party to such a funds transfer that we have reported, or intend to report it.

Bank Transaction Settlement Time

We expect our Bank(s) to process and settle ACH and Wire transfers in an ordinary manner, as if such transfers were initiated by any customer of our Bank(s). Our CEO will review, at least annually, the transaction settlement performance of our Bank(s).

Employee Fingerprinting and Background Checks

We arrange for the fingerprinting of all Employees who approve, review or facilitate the transfer of User funds. We retain processed fingerprint cards and accompanying information for the duration of the Employee's employment with our Organization and for a minimum of three (3) years after the end of his or her employment with our Organization. All Employees sign a consent form authorizing us to conduct an initial Background Check and to conduct, with or without the Employee's knowledge, periodic Background Checks during the course of the Employee's employment with our Organization.

CONFIDENTIAL

Last revised - May 21, 2017

CUSTODY OF FIAT FUNDS

Policy

Our Organization holds Users' fiat funds in one or more of our Omnibus Bank Accounts at one or more of our Banks. Our Employees do not directly handle User fiat funds, but our Organization controls our Omnibus Bank Accounts holding Users' fiat funds. The balance of User's fiat funds are recorded in our Exchange Ledger and reflected in each User's Fiat Account.

Safeguarding. All User fiat funds are held in our Omnibus Bank Accounts, which are segregated and legally distinct from our Organization's business, operating and reserve accounts.

Procedures

Principal Bank

As of the date of this Manual, our Organization's principal Bank is Silvergate Bank, a California-based full-service commercial bank. Silvergate Bank is headquartered at 4275 Executive Square, Suite 800 La Jolla, CA 92037.

Instructions to our Bank(s) are delivered, after receipt of User instructions via our Online Platform, either automatically by our computer systems or, under certain circumstances, manually by our Employees.

Omnibus Bank Account Review

Prior to allowing Users to deposit fiat funds at one of our Omnibus Bank Accounts, our CCO verifies that an Omnibus Account for User fiat funds has been established at such Bank and is able to receive User fiat deposits.

CONFIDENTIAL

Last revised - May 21, 2017

CUSTODY OF DIGITAL ASSETS

Policy

Our Organization has direct custody of Users' Digital Assets. We maintain custody of Digital Assets in our Pooled Accounts through the storage of private keys that permit transfers from Digital Asset addresses. The balance of User's Digital Assets are recorded in our Exchange Ledger and reflected in each User's Digital Asset Account.

Depository Account. All User's Digital Assets not held in Segregated Accounts (as defined below), are held in our Pooled Accounts, which are segregated from our Organization's business, operating, and reserve Digital Asset accounts (each, a "Depository Account").

Segregated Account. Our custodial service offers Users the ability to hold Digital Assets in one or more segregated Digital Asset addresses (each, a "Segregated Account") in our Cold Storage System, which are segregated from any and all other Digital Assets held by our Organization and are directly verifiable via the applicable blockchain. This is different from a standard Depository Account (as defined above).

Procedures

Three-Tiered Storage System

Our Organization's Digital Assets (including User's funds) are stored and secured in our three-tiered Digital Asset storage system:

- **Hot Storage** — The first tier ("Hot") that comprises our Hot Wallet system ("Hot Wallet System"), holds approximately 5%² of Users' total Digital Assets on deposit and is Internet-connected, meaning that access to private keys is available through computers directly or indirectly connected to the Internet. Our Hot Wallet System is designed to process Digital Asset withdrawals for Users on a near real-time basis.
- **Cold Storage** — The second tier ("Cold") that comprises the first part of our Cold Storage System, holds approximately 15% of Users' total Digital Assets on deposit and uses offline (i.e., air-gapped, non Internet-connected) dedicated cryptographic hardware security modules ("HSMs," each a "Signer") to store its private keys. All of our HSMs are stored in geographically distributed, access-controlled physical storage facilities (each, a

² The targeted 5%-15%-80% distribution of Digital Assets in custody are end state targets, and will be achieved once sufficient total funds are in custody to satisfy regular fluctuations in User deposits and withdrawals from the Hot wallet with 5% of total funds held. As of Q1 2017, we have not yet reached an asset level that allows this ratio to be achieved.

CONFIDENTIAL

Last revised - May 21, 2017

"Storage Facility"). Our Cold Storage utilizes a "M-of-N" multisignature ("Multisig") signing design, with a specific 2-of-3 implementation. In addition, our Cold Storage Facilities contain an encrypted backup of the master key used for deriving our Hot Wallet System, providing a recovery strategy should our Hot Wallet System become unavailable. Our Cold Storage is intended for the long-term storage of Digital Assets. We can generally process Digital Asset withdrawals from our Cold Storage within one (1) business day.

- **Cryo Storage** — The third tier ("Cryo") that comprises the second part of our Cold Storage System, holds the remaining 80% of Users' total Digital Assets on deposit and also uses offline (i.e., air-gapped, non Internet-connected) Signers to store its private keys. All of our Signers are stored in Storage Facilities. Our Cryo Storage utilizes a Multisig signing design, with a specific 2-of-6 implementation. In addition, some Cryo Storage Facilities contain a backup clone of a Signer. Our Cryo Storage is intended to be used for the long-term storage of Digital Assets. We can generally process Digital Asset withdrawals from our Cryo Storage within two (2) business days.

Digital Asset Allocation

Our Organization maintains a percentage of Digital Assets held in our Hot Wallet System; management determines the percentage to be held on a periodic basis. Please refer to the 'Hot Omnibus Management' section of our **Digital Asset Runbook** for procedural information on Digital Asset Allocation between our Hot Wallet System and Cold Storage System.

Segregated Account Management

Please refer to the 'Segregated Account Management' section of our **Digital Asset Runbook** for procedural information on the management of Segregated Accounts.

Storage Facility Access / Operation of Signers

Only Employees who are designated as custodians for our Cold Storage System (each, a "Token Holder") are permitted to access the Storage Facilities utilized by our Cold Storage System. All Token Holders have unique credentials required to operate the Signers of our Cold Storage System. Each Token Holder is subject to: (i) our Token Holder Policy; (ii) heightened Background Checks; and (iii) may be bonded.

We maintain a Storage Facility log ("Storage Facility Log") that keeps track of every visit made by a Token Holder to a Storage Facility. Each Token Holder is responsible for filling out the Storage Facility Log fully and completely for every visit he or she makes to a Storage Facility. Failure to do so is a direct violation of our Token Holder Policy. See the 'Storage Facility Log' subsection of the 'Token Holder Policy' section below for more information.

CONFIDENTIAL

Last revised - May 21, 2017

Please refer to the 'Operation of Signers' subsection of the 'Cold Storage System' section of our **Digital Asset Runbook** for procedural information on Storage Facility access and operation of Signers.

Storage Facility Review

Prior to storing a Signer in a Storage Facility, our CSO must approve such Storage Facility and verify that an account for our Organization at such Storage Facility has been established.

Proof of Control

Please refer to the 'Proof of Control' subsection of the 'Cold Storage System' section of our **Digital Asset Runbook** for procedural information on proof of control.

CONFIDENTIAL

Last revised - May 21, 2017

TOKEN HOLDER POLICY

Policy

Our Token Holder policy ("Token Holder Policy") sets forth the policies and procedures regarding our Token Holders who custody one or more tokens (each, a "Token") that are necessary to access and operate our Cold Storage System.

Procedures

Pursuant to our Organization's Security Policy, a percentage of Users' Digital Assets are held in our offline (i.e., air-gapped, non Internet-connected) Cold Storage System, which is comprised of HSMs that are stored in Storage Facilities. Access to Storage Facilities is restricted to Token Holders.

Appointment and Termination

Each Token Holder has been appointed by our CEO and President, in consultation with our CSO. Upon acceptance, Each Token Holder has agreed to serve as a Token Holder until the earlier of the following: (i) he or she provides our CSO with at least ninety (90) days prior written notice that he or she is unable or unwilling to continue to fulfill his or her responsibilities as outlined by this Token Holder Policy; (ii) he or she has resigned or been terminated with or without cause, as defined in each Token Holder's respective Employment Agreement; or (iii) our CEO and President, collectively, decide to remove a Token Holder from being a Token Holder for any reason whatsoever, with or without cause. Notwithstanding anything to the contrary herein, the confidentiality provision of this Token Holder Policy shall survive the termination of any Token Holder.

Responsibilities

- **Custody** — Each Token Holder has custody of one or more Tokens, all of which are the property of our Organization. With the exception of our CEO and President, or when otherwise approved and instructed to by our CSO, each Token Holder agrees to never give custody of any of his or her Tokens to anyone else at any time. Any Token Holder instructed to hold custody of one or more Tokens other than his or her own, agrees not to attempt to use any such Tokens.
- **PIN** — Each Token Holder is required to create a personal identification number ("PIN") for each Token that he or she operates. Each PIN must be a unique code that a Token Holder is not using for any other purpose other than for applications related to our Cold Storage System. The same PIN may be used for one or more Tokens that a Token

CONFIDENTIAL

Last revised - May 21, 2017

Holder operates, unless otherwise directed by the CSO. A PIN that is currently in use or has been previously used as a PIN or password on any other system, including online websites or payment systems such as ATM cards or to authenticate to any other Organization service or application, may not be reused. Lastly, a PIN must be truly unique, strong and not easily derived from public knowledge or readily available or easily-obtained information about you, someone close to you (e.g., a family member or significant other), or any other Employee or Token Holder. Token Holders may change their PIN, as long as the new PIN also meets all of the requirements described above.

With the exception of our CEO and President, as described herein, or when otherwise approved and instructed to by our CSO, each Token Holder agrees never to share any of his or her Token-related PINs with anyone else at any time. In addition, if an Token Holder decides to store his or her PIN in tangible form (e.g., in writing or encrypted on a form of digital storage media), it must be stored in a different and secure location from its Token, subject to our CSO's approval.

- **Storage Location** — Each Token Holder is expected to use reasonable best efforts to store each Token in a secure storage location (each, a "Storage Location") that is readily accessible to him or her, such as a personal safe (if, and only if, its specifications are approved by our CSO) or a safety deposit box at a bank. Each Storage Location must be approved by our CSO. If any Storage Location is not accessible at all times (i.e., twenty-four (24) hours a day, seven (7) days per week and three hundred and sixty-five (365) days per year), then each Token Holder must advise our CSO of such access limitations. Our CSO, or designee, securely documents each Token Holder's Storage Location and notes any such access limitations. Absent extraordinary circumstances, it is the obligation of each Token Holder to inform the CSO of (i) any changes to any Storage Location prior to moving any Token and (ii) any changes to accessibility of a given Storage Location. When a Token is not in its Storage Location, its Token Holder must have direct possession of it at all times, unless otherwise approved and instructed to by the CSO.
- **Usage** — No Token Holder may attach any Token to any computer or device other than the specified HSMs associated with our Cold Storage System and located in a Storage Facility.
- **Notifications** — Each Token Holder agrees to notify our CSO as soon as possible or as permitted by law and in writing, if any of the following occur: (i) any Token has been misplaced, lost, or stolen; (ii) any PIN has been forgotten for any Token; or (iii) the confidentiality of any PIN has been compromised for any Token. Failure to notify our CSO of any of the above, may result in our Organization imposing sanctions, up to and including termination of your employment or your services.

CONFIDENTIAL

Last revised - May 21, 2017

Participation in Operations

Each Token Holder is required to participate in our Cold Storage System operations from time to time and whenever necessary. If a Token Holder is asked to visit a Storage Facility and operate one of his or her Tokens, such Token Holder must use reasonable best efforts to do so in a timely manner and within our Organization's Service Level Agreement ("SLA") for that operation. If a Token Holder knows that he or she will not be available (e.g., on vacation or otherwise) for more than a twenty-four (24) hour period, such Token Holder must notify our CSO in advance via the Organization's established Vacation Policy notification protocol (see **Policies and Procedures** manual 'Paid Vacation' section).

Access Controls

Each Token Holder understands that he or she is never permitted to go to any Storage Facility alone (i.e., all Storage Facilities are "no-lone zones") for any reason whatsoever since at least two (2) Token Holders with hardware Tokens for authentication are required as part of our Cold Storage System's access controls design. In addition, if any Token Holders are family members or in a relationship that could be a potential conflict, such Token Holders will be issued clones of the same Token. Such clones cannot be combined to create the required quorum of two (2) Token Holders.

Storage Facility Log

Each Token Holder is required to log every visit he or she makes to a Storage Facility in our Storage Facility Log. Each Token Holder has access to our Storage Facility Log which is stored and secured in our cloud storage system. It is the sole responsibility of each Token Holder to fill out the Storage Facility Log fully and completely for every visit he or she makes to a Storage Facility. Failure to do so is a direct violation of our Token Holder Policy.

Confidentiality

Any and all information related to our Organization's Tokens is considered confidential, including, but not limited to, information such as the identity of a Token Holder or the location of a Storage Facility. Such confidential information shall only be disclosed on a strictly need-to-know basis and **never without the prior written consent of our CSO**. Furthermore, a Token Holder may never attempt to duplicate, reverse engineer, or otherwise attempt to extract the authentication credentials of or any information from any Token.

Transfer of Token Custody

CONFIDENTIAL

Last revised - May 21, 2017

If a Token Holder's relationship with our Organization ends for any reason, he or she must immediately return all Tokens in his or her custody to the CSO, or designee. If our CEO, President, or CSO request that a Token Holder return any or all of his or her Tokens for any reason, the Token Holder must immediately return all of the requested Tokens in his or her custody to the CSO, or designee. The Transfer of custody of a Token requires that a Token Holder hand-off his or her Token in-person to our CSO, or designee. In addition, the Token Holder must convey, in-person or via a secure band of communication, the PIN for any of his or her transferred Tokens to his or her designated Token Holder replacement.

Amendments

Our Token Holder Policy may only be amended in writing by our CSO, in consultation with our CEO and President. Any update to our Token Holder Policy will be circulated in writing to and acknowledged in writing by each Token Holder.

Certification

By executing the signature page attached hereto as **Appendix 3**, you certify and acknowledge that you have (i) received a copy of our entire Token Holder Policy and (ii) have read and understand all of its provisions and your responsibilities thereunder, all of the foregoing a condition of being a Token Holder and any violation thereof a cause for sanctions, up to and including termination of your employment or your services with our Organization.

CONFIDENTIAL

Last revised - May 21, 2017

EXCHANGE LEDGER

Policy

It is the policy of our Organization to utilize controls and procedures regarding the adjustment of funds allocated to User accounts.

Certain User account adjustments require approval from the **Management** Approval Group (as defined below).

Prompt settlement of User executed trades is a priority of our Organization. We will notify affected Users if the settlement of an executed trade is delayed and/or a manual adjustment is required.

Procedures

Approval Groups

Gemini Admin — Certain Employees have access to our Admin. Some of these Employees are members of the following Approval Group as defined below:

- **Management** — Our President, CEO, and CCO.

Approval Design

The following approvals are required for an adjustment to our Exchange Ledger:

- A **credit** or **debit** of fiat funds or Digital Assets to a User's Gemini Account can be submitted by any one (1) Employee with Admin access, but must be approved by one (1) member of the **Management** group.

All approval actions, as described above, are recorded and visible to Employees with Admin access.

Pooled Accounts

We use a book-entry system to track the fiat funds and Digital Asset balance of each Gemini Account in our Exchange Ledger. Our book-entry system is an automated system that is maintained in a master electronic file. We facilitate and settle trades, deposits and withdrawals through updates to our Exchange Ledger (e.g., debiting and crediting User Fiat Account and Digital Asset Account balances to reflect executed trades).

CONFIDENTIAL

Last revised - May 21, 2017

Securing, Maintaining and Backing Up

Our Chief Security Officer ("CSO") will review, at least annually, the processes by which our Exchange Ledger is secured, maintained, updated (e.g., edited to reflect the settlement of trades, deposits, withdrawals and adjustments) and backed up.

Records

All adjustments to the Exchange Ledger are maintained in the records of our Organization for a period of at least seven (7) years. Adjustments to the Exchange Ledger that changes a User's Gemini Account balance are reflected in such User's Fiat Account and/or Digital Asset Account.

Backups

Backups of our Exchange Ledger are generated daily and stored for a period of not less than ninety (90) days.

CONFIDENTIAL

Last revised - May 21, 2017

TRADE ERRORS & MODIFICATIONS

Policy

Trade Errors. Errors may occur on our Exchange in the order entry, order matching, or trading process (each, a "Trade Error"). Examples of such Trade Errors may include, but are not limited to:

- Data corruption in the authentication process for order entry or order matching that results in an incorrect purchase or sale order (each, an "Order"); or
- System failure that results in the incorrect population of the Order Book or incorrect application of the Exchange Trading Engine; or
- A trade (each, a "Trade") that is empirically disruptive to an orderly market and, therefore, represents a false and misleading view of the market.

Clerical mistakes that have an impact solely on recordkeeping are not treated as Trade Errors. Trade Errors that are the result of *User actions or inaction* (including, without limitation, actions of a third party accessing a User's account using such User's login credentials) are generally not subject to modification and Users bear the risk of such Trades Errors, pursuant to our User Agreement.

Erroneous Trades. We reserve the right to reverse and/or modify one or more Trades (each, an "Erroneous Trade") in the event of:

- Any disruption or malfunction in the operation of any electronic communications, trading facilities, storage facilities, recording mechanisms or other components of or integral to Gemini or of Digital Assets;
- Any other significant business disruption (each, an "SBD") to Gemini or Digital Assets, whereby the nullification or modification of one or more Trades may be necessary for the maintenance of a fair and orderly market and/or the protection of our Users and/or the public interest; or
- Any Trade that we deem clearly erroneous in our sole discretion.

If an Erroneous Trade occurs, members of the **Management Approval Group** (as defined below) may review such Erroneous Trade and declare it null and void. Absent extraordinary circumstances, any modification made by the **Management Approval Group** related to an Erroneous Trade, will be taken within three (3) business days of detection of the Erroneous Trade. We will notify any Users involved and/or impacted as soon as practicable.

CONFIDENTIAL

Last revised - May 21, 2017

Erroneous Orders. We reserve the right to cancel one or more Orders (each, an "Erroneous Order") in the event of:

- Any disruption or malfunction in the operation of any electronic communications, trading facilities, storage facilities, recording mechanisms or other components of or integral to Gemini or of Digital Assets;
- Any other SBD to Gemini or Digital Assets, whereby the nullification of modifications of one or more Orders may be necessary for the maintenance of a fair and orderly market and/or the protection of our Users and/or the public interest;
- Any Order with the potential to move the market price by more than twenty percent (20%) in either direction or is otherwise clearly erroneous; or
- Any Order that we deem clearly erroneous in our sole discretion.

If an Erroneous Order occurs, members of the **Management** Approval Group (as defined below) may review such Erroneous Order and declare it null and void. Absent extraordinary circumstances, any modification made by the **Management** Approval Group related to an Erroneous Order, will be taken within three (3) business days of detection of the Erroneous Order. We will notify any Users involved and/or impacted as soon as practicable.

Organization Trade Errors. In the event that our Organization is responsible for a Trade Error, it is our policy that we may, at the discretion of our CCO and senior management, roll back such Organization Trade Error, if possible. If an Organization Trade Error is not able to be rolled back without inequitably imposing a burden on one or more Users, we may, at the discretion of senior management, decide to make trade participants whole. Senior management will determine whether a Trade Error has resulted from the gross negligence of our Organization. In the absence of the gross negligence of our Organization, losses from Trade Errors are borne by the affected Users.

Trade Entry Failure. When a Trade Error has occurred (whether as a result of User error or Organization error) and such Trade Error either (i) prevents the settlement of an applicable Trade after order matching; or (ii) is discovered prior to order matching, we will cancel the applicable Trade or Order.

Procedures

CONFIDENTIAL

Last revised - May 21, 2017

Approval Groups

Gemini Admin — Certain Employees have access to our Admin. Some of these Employees are members of the following Approval Group as defined below:

- **Management** — Our President, CEO, and CCO.

Approval Design

The following approvals are required for a trade modification:

- A **trade modification** can be submitted by any one (1) Employee with Admin access, but must be approved by three (3) members of the **Management** group.

All approval actions, as described above, are recorded and visible to Employees with Admin access.

Discovery & Reporting of Errors

An Organization Trade Error must be reported to the CCO as soon as reasonably practical.

Reporting to Users

An Organization Trade Error that affects a User's Trade or Order shall be reported to such User and recorded in such User's account file by the Customer Service Team.

Pre-Settlement Correction

A Trade Error that is discovered before settlement (i.e., an Erroneous Order), will generally be automatically cancelled (based on logic).

Post-Settlement Correction

A Trade Error that is discovered after settlement (i.e., an Erroneous Trade), will generally not be corrected if it was caused by a User and did not prejudice any trading counterparty who did not cause the Trade Error. An Organization Trade Error that is discovered after settlement, may be corrected, when possible, by rolling back the Trade Error through the entry of one or more additional transactions that reverse the effect of the Trade Error and, if applicable, affect the intended result of the initial Trade.

CONFIDENTIAL

Last revised - May 21, 2017

Appendix 1: Initial Certification

IN WITNESS WHEREOF, I acknowledge that I have received a copy of our Organization's *Policies and Procedures - Funds Transfer, Ledger, and Custody* manual ("Manual"), and represent that:

1. I have read this Manual and understand the individual policies and procedures included therein;
2. I understand that our Organization may impose sanctions, up to and including termination of employment, for violation of any provision of this Manual; and
3. I will comply with this Manual (and each of our Organization's policies and procedures) in all respects.

Signature: _____

Name: _____

Title: _____

Date: _____

CONFIDENTIAL

Last revised - May 21, 2017

Appendix 2: Annual Certification

IN WITNESS WHEREOF, I certify that I have reread, understand and will comply with this *Policies and Procedures - Funds Transfer, Ledger, and Custody* manual ("Manual") in all respects going forward. I also certify that during the past calendar year, I have complied with this Manual in all respects. Any exceptions to this Manual that I have made during the past calendar year are described in the comments section below. I acknowledge that by leaving the comment section below blank, I am certifying that I have not made any exceptions to any part of this Manual.

Signature: _____

Name: _____

Title: _____

Date: _____

Comments:

CONFIDENTIAL

Last revised - May 21, 2017

Appendix 3: Token Holder Certification

IN WITNESS WHEREOF, I acknowledge that I have received a copy of our Organization's *Token Holder Policy* ("Policy") and represent that:

1. I agree to be a Token Holder of our Organization (in accordance with the schedule below);
2. I understand and agree that any Token in my possession and/or that requires the use of my PIN is the property of our Organization;
3. I will keep the fact that I am a Token Holder confidential and will not disclose information regarding any other Token Holder or Storage Facility;
4. I have read this Policy and understand the individual policies and procedures included therein;
5. I understand that our Organization may impose sanctions, up to and including termination of employment, for violation of any provision of this Policy;
6. If I have made an exception to any part of this Policy I will notify the CSO immediately; and
7. I will comply with this Policy in all respects.

Signature: _____

Name: _____

Title: _____

Date: _____